UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,178	08/14/2001	Donald P. Matthews JR.	BRCMP008/BP-1567	8980

23363 7590 08/31/2005

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,178	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 26-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 26-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-10, and 26-40 are pending.

Response to Arguments

1. Applicant's arguments, see pages 14-15, filed 6/10/2005, with respect to the rejection(s)of claim(s) 1-10 under 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made with Caputo (U.S. Patent 5,778,071) in view of SSL3spec, TLSspec, Kaplan, and/or Gaytan (U.S. Patent 5,638,367).

Claim Objections

2. Claims 4, 7, and 37 are objected to because of the following informalities:

- Claim 4, lines 2-3 recite the limitation "the IS cryptography operations". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, it has been construed as "the cryptography operations".
- Claim 7, line 2 recites the limitation "calculation of a pad length". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, it has been construed as "a calculation of a pad length".
- Claim 37, lines 1-2 reads "wherein aligning comprises comprising aligning", which should be "wherein aligning comprises aligning".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 8-10, 26, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo (U.S. Patent 5,778,071) in view of SSL3spec (Freier et al., "The SSL Protocol Version 3.0", 11/18/1996, pp. 1-12, obtained from http://wp.netscape.com/eng/ssl3/draft302.txt).

Regarding Claim 1,

Caputo discloses a method of processing network security protocol data packets, comprising:

Providing a cryptography processing architecture on a chip (Column 17, line 57 to Column 18, line 9);

Passing network security protocol data for both authentication and cryptography operations from a source to the chip (Column 15, lines 25-30);

Conducting, in hardware, authentication and encryption operations on the network security protocol data (Column 17, line 57 to Column 18, line 9); and

Passing the crypto-processed network security protocol data from the chip to the source (Column 15, lines 25-30);

Wherein the network security protocol data is passed between the chip and the source in a single pass (Column 17, line 57 to Column 18, line 9).

Caputo does not disclose that the network security protocol data is non-pre-padded.

SSL3spec, however, discloses that the data is non-pre-padded network security protocol data (Pages 3-4, Section 1; and Page 10, Section 5.0). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the crypto device of Caputo in order to gain cryptographic security between two parties and interoperability between differently coded programs (Page 4, Sections 2.1, 2.2, and 2.3).

Regarding Claim 2,

SSL3spec discloses that the network security protocol is SSL (v3) (Pages 3-4, Section 1; and Page 10, Section 5.0).

Regarding Claim 8,

Caputo discloses that conducting, in hardware, authentication and encryption operations on the network security protocol data comprises feeding back a MAC value calculated during authentication operations for processing in the encryption

operations (Column 11, line 60 to Column 12, line 13; and Column 18, lines 1-9).

Regarding Claim 9,

Caputo discloses that the encryption operations further include decryption operations (Column 17, lines 57-67).

Regarding Claim 10,

Caputo discloses that conducting, in hardware, authentication and decryption operations on the network security protocol data comprises feeding back decrypted data for processing in the authentication operations (Column 11, line 60 to Column 12, line 13; and Column 17, lines 57-67).

Regarding Claim 26,

Caputo discloses a method of processing network security protocol data packets, comprising:

Receiving, at a chip, security protocol data for both authentication and cryptography operations from a source (Column 15, lines 25-30);

Aligning, at the chip, the received network security protocol data to provide aligned network security protocol data (Column 9, lines 46-61);

Conducting, at the chip, authentication operations and at least one of encryption operations and decryption operations on the aligned network security protocol data to provide processed

network security protocol data (Column 17, line 57 to Column 18, line 9); and

Passing the processed network security protocol data from the chip to the source (Column 15, lines 25-30);

Wherein the network security protocol data is passed between the chip and the source in a single pass (Column 17, line 57 to Column 18, line 9).

Caputo does not disclose that the network security protocol data is non-pre-padded.

SSL3spec, however, discloses that the data is non-pre-padded network security protocol data (Pages 3-4, Section 1; and Page 10, Section 5.0). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the crypto device of Caputo in order to gain cryptographic security between two parties, interoperability between differently coded programs, and extensibility to other protocols and methods (Page 4, Sections 2.1, 2.2, and 2.3).

Regarding Claim 31,

Caputo discloses that the authentication operations comprise authenticating at least a portion of the aligned network security protocol data (Column 11, line 60 to Column 12, line 13).

4. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of SSL3spec, further in view of TLSspec (Dierks et al., "The TLS Protocol Version 1.0", 10/28/1997, pp. 1-12, obtained from http://ww.umk.pl/~mgw/internet-drafts/draft-ietf-tls-protocol-04.txt).

Caputo as modified by SSL3spec does not disclose the TLS protocol.

TLSspec, however, discloses that the network security protocol is TLS (Pages 3-4, Section 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of TLSspec into the crypto device of Caputo as modified by SSL3spec in order to gain extensibility to other protocols and methods (Pages 4-5, Sections 2.1, 2.2, and 2.3).

5. Claims 4-7, 29, 30, 32, 33, and 35-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of SSL3spec, further in view of Kaplan (U.S. Patent 6,704,871).

Regarding Claim 4,

Caputo as modified by SSL3spec does not disclose simultaneously with conducting the cryptography operations on the network security protocol data, pre-loading network security protocol data from a second non-pre-padded network security protocol packet onto the chip.

Kaplan, however, discloses simultaneously with conducting the cryptography operations on the network security protocol data, pre-loading network security protocol data from a second non-pre-padded network security protocol packet onto the chip (Column 37, lines 47-58). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the crypto chip of Kaplan into the crypto device of Caputo as modified by SSL3spec in order to obtain fast processing through paralleled and pipelined operations and to facilitate peak encrypt/decrypt performance (Column 41, lines 17-19).

Regarding Claim 5,

Kaplan discloses simultaneously with conducting the encryption operations on the network security protocol data, conducting in hardware, authentication operations on the network security protocol data from the second network security protocol packet (Column 37, lines 47-58).

Regarding Claim 6,

Kaplan discloses that conducting, in hardware, authentication and encryption operations on the non-pre-padded network security protocol data comprises conducting padding and alignment operations on the chip (Column 41, lines 16-51).

Regarding Claim 7,

Kaplan discloses that a calculation of a pad length for padding operations is conducted by a pad engine component of the chip architecture (Column 41, line 16 to Column 42, line 3).

Regarding Claim 29,

Caputo discloses storing the aligned network security protocol data in a FIFO to accumulate a predefined amount of data before commencing the authentication operations and the at least one of encryption operations and decryption operations (Column 9, lines 46-61).

Kaplan also discloses storing the aligned network security protocol data in two FIFOs (one for cryptographic operations and one for authentication operations) to accumulate a predefined amount of data before commencing the authentication operations and the at least one of encryption operations and decryption operations (Column 38, lines 50-57).

Regarding Claim 30,

Kaplan discloses that the predefined amount of data comprises 512 bits (Column 38, lines 50-57).

Regarding Claim 32,

SSL3spec discloses that at least a portion of the aligned network security protocol data comprises Content Type, Length, and Data (Page 10, Section 5.0).

Regarding Claim 33,

Kaplan discloses aligning, for encryption operations, at least a portion of the received non-pre-padded network security protocol data and the authenticated at least a portion of the aligned network security protocol data to provide the aligned network security protocol data for the encryption operations (Column 39, lines 26-42).

Regarding Claim 35,

Kaplan discloses that aligning, for encryption operations, comprises padding (Column 39, lines 26-37).

Regarding Claim 36,

Kaplan discloses storing the aligned network security protocol data for the encryption operations in a FIFO to accumulate a predefined amount of data before commencing the encryption operations (Column 40, lines 43-52).

Regarding Claim 37,

Kaplan discloses aligning, within a decryption path, the received non-pre-padded network security protocol data to provide the aligned network security protocol data for the decryption operations (Column 39, lines 26-42).

Regarding Claim 38,

Caputo discloses decrypting the aligned network security protocol data for the decryption operations and providing at least a

portion of the decrypted data for the authentication operations (Column 17, lines 57-67).

Regarding Claim 39,

Kaplan discloses aligning the at least a portion of the decrypted data for the authentication operations (Column 41, lines 16-51).

Regarding Claim 40,

Kaplan discloses performing at least a portion of the authentication operations and at least a portion of the encryption operations and decryption operations in parallel (Column 37, lines 47-58).

6. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of SSL3spec, further in view of Gaytan (U.S. Patent 5,638,367).

Regarding Claim 27,

Caputo as modified by SSL3spec does not disclose removing non-valid data from the received data.

Gaytan, however, discloses removing non-valid data from the received data (Column 1, line 62 to Column 2, line 29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data packing system of Gaytan into the crypto device of Caputo as modified by SSL3spec

in order to gain better throughput and performance by only sending valid data past the buffer.

Regarding Claim 28,

Gaytan discloses packing the data (Column 1, line 62 to Column 2, line 29).

7. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of SSL3spec and Kaplan, further in view of Gaytan.

Caputo as modified by SSL3spec and Kaplan does not disclose that aligning comprises removing non-valid data.

Gaytan, however, discloses that aligning comprises removing non-valid data (Column 1, line 62 to Column 2, line 29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data packing system of Gaytan into the crypto device of Caputo as modified by SSL3spec in order to gain better throughput and performance by only sending valid data past the buffer.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The

fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER